

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Digital Devices listed in Attachment A, obtained from William
Woodward, or his residence located at 220 East Warren
Street in Cadiz, Ohio, currently in possession of the
Cincinnati FBI Office located at 2012 Ronal Regan Drive
in Cincinnati, Ohio

Case No. 2:21-mj-658

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

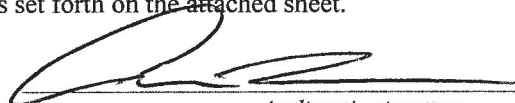
*Code Section**Offense Description*

18 U.S.C. §§ 2252, and 2252A Distribution, transmission, receipt, and/or possession of visual depictions of a minor engaged in sexually explicit conduct and/or child pornography

The application is based on these facts:

See attached affidavit incorporated herein by reference.

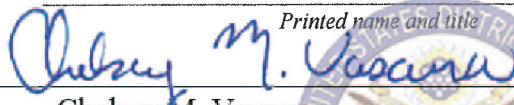
- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

FBI SA Andrew McCabe

Printed name and title

Sworn to before me and signed in my presence.

Date: October 12, 2021City and state: Columbus, Ohio

 Chelsey M. Vascara
 United States Magistrate Judge
Judge's signature
Chelsey M. Vascara, U.S. Magistrate Judge
Printed name and title

**UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO,
EASTERN DIVISION**

IN THE MATTER OF THE SEARCH OF:

Case No: 2:21-mj-658

**Digital devices as listed in Attachment A that were
obtained from William WOODWARD, or his residence
located at 220 East Warren Street in Cadiz, OH,
and are currently in the possession of the Cincinnati FBI,
located at 2012 Ronald Reagan Drive in Cincinnati, Ohio.**

Magistrate Judge: Vascura

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrew D. McCabe, a Special Agent with the Federal Bureau of Investigation (FBI),
being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, Cambridge Resident Agency and I have been a Special Agent since September 2010. During my tenure as an FBI Special Agent, I have investigated numerous crimes including, but not limited to, bank robbery, drug trafficking, racketeering, kidnapping, violent extremism, and crimes against children.
2. While performing my duties as a Special Agent, I have participated in various investigations involving computer-related offenses and have executed search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. As part of my duties as a Special Agent, I investigate various criminal child exploitation offenses, including those in violation of 18 U.S.C. §§ 2251, 2252, and 2421 *et seq.*
3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have not withheld any evidence or information which would negate probable cause. I have set forth only the facts necessary to establish probable cause for a search warrant for the content of two digital devices that were seized from the person of William **WOODWARD** or his residence located at 220 E. Warren Street in Cadiz, Ohio 43907 which are currently held in the custody of the Cincinnati FBI Field Office, located at 2012 Ronald Reagan Drive in Cincinnati, Ohio 45236 (hereinafter referred to as the **SUBJECT DEVICES**).
5. The **SUBJECT DEVICES** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits and evidence of violations of 18 U.S.C. §§ 2252 and 2252A – the distribution, transmission, receipt, and/or possession of visual depictions of minors engaged in sexually explicit conduct (hereinafter “child pornography”). I am requesting authority to search the entire content of the **SUBJECT DEVICES**, wherein the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.
7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any

child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

8. The term "child pornography"¹, as it is used in 18 U.S.C. § 2252A, is defined pursuant to 18 U.S.C. § Section 2256(8) as "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually conduct.
9. The term "sexually explicit conduct", is defined pursuant to 18 U.S.C. § 2256(2)(A) as "actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person." Pursuant to 18 U.S.C. § 2256(2)(B), "sexually explicit conduct" when used to define the term child pornography, also means "(i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (ii) graphic or lascivious simulated; (I) bestiality; (II) masturbation; or (III) sadistic or masochistic abuse; or (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person."
10. The term "minor", as used herein, is defined pursuant to Title 18, U.S.C. § 2256(1) as "any person under the age of eighteen years."

¹ The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

11. The term “visual depiction,” as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”
12. “Graphic” when used with respect to a depiction of sexually explicit conduct, means that viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10)).
13. The term “computer”² is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
14. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).
15. “Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.
16. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.
17. As it is used throughout this affidavit and all attachments hereto, the term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or

² The term “computer” is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also to internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

optical media.

IV. BACKGROUND REGARDING DIGITAL DEVICES, THE INTERNET AND MOBILE APPLICATIONS

18. I know from my training and experience that computer hardware, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.
19. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.
20. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.
21. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including

"MPG/MPEG" (Moving Pictures Experts Group) files.

22. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 32GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred, it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.
23. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service

Providers (“ISPs”). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs’ servers or cellular network; remotely store electronic files on their customers’ behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol (“IP”) addresses³ and other information both in computer data format and in written record format.

24. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user’s true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.
25. It is often possible to recover digital or electronic files, or remnants of such files, months or even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later

³ The IP address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most ISPs control a range of IP addresses. When mobile devices connect to the Internet they are assigned an IP address either by the residential/commercial WiFi ISP or the cellular ISP. The IP address assignments are controlled by the respective provider.

using readily available forensic tools. When a person “deletes” a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

26. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.
27. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
28. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as “apps,” are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such “apps” include Facebook Messenger, Text Now, KIK messenger service, and Instagram.
29. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate

law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
 - a) Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
 - b) Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.
31. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU) as well as all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

VI. INVESTIGATION AND PROBABLE CAUSE

32. On September 23, 2021, Witness One contacted the Cadiz Police Department (CPD) to make a report regarding a child exploitation offense. More specifically, Witness One indicated that the night before, on September 22, 2021, Witness One had observed William WOODWARD using a laptop computer to view a video of a young child performing sexual acts. Witness One indicated that he/she was at WOODWARD's residence, located at 220 East Warren Street in Cadiz, Ohio when he/she went to knock on WOODWARD's bedroom door. Witness One observed that the bedroom door was open and observed WOODWARD masturbating to a video containing child pornography which Witness One estimated to depict an approximately nine-year-old child.
33. Based on this information, CPD officers relocated to WOODWARD's residence on September 23, 2021. WOODWARD answered the door and agreed to speak with law enforcement outside. CPD informed WOODWARD that they were following up with a complaint involving WOODWARD's child exploitation activities and asked WOODWARD if he had a laptop computer. WOODWARD admitted to owning a computer and gave the officers consent to enter his residence. WOODWARD took the officers to his bedroom where he voluntarily turned over a Gateway Laptop Computer and Black LG Cellular Telephone, the **SUBJECT DEVICES**. WOODWARD made a statement to CPD that "[CPD] knew what was going to be on them," indicating to law enforcement that WOODWARD was confirming the presence of child pornography on the **SUBJECT DEVICES**.
34. WOODWARD was subsequently placed under arrest for Pandering Sexually Oriented Matter Involving a Minor in violation of Ohio Revised Code Section 2907.321 and advised of his Miranda Rights. Law enforcement then transported WOODWARD to the Cadiz Police Department for a further interview. At the Cadiz Police Department, WOODWARD was advised of his Miranda Rights a second time and signed a waiver on September 23, 2021 at 9:35am indicating his intent to waive those rights. WOODWARD was then interviewed by CPD and that interview was recorded both audially and visually. A copy of that interview was provided to your affiant.
35. During the interview with CPD, WOODWARD admitted to having images of minor girls on the **SUBJECT DEVICES** and further admitted to viewing videos of minor females

engaged in sex acts. WOODWARD also indicated that the videos he viewed depicted minor females as young as approximately ten years old engaging in sexual acts.

36. In that same interview, WOODWARD provided the password of both **SUBJECT DEVICES** to law enforcement. When CPD entered WOODWARD's password into the Gateway Laptop to ensure it was correct, they immediately observed a video on the laptop screen which depicted a naked prepubescent female. The video was titled, "2010-9TO-SUZIQ-COMPIL-FUCKS-PUSSY-ON-TABLE-VEWRS-SOUND-HQ-11M52S-MKV. Law enforcement took five photos of the video observed on the Gateway Laptop and provided them to your affiant. The images are described as follows:

- Image One and Image Two depicted a prepubescent female minor, approximately nine years old (hereinafter Minor Victim), with her nude breasts exposed wearing white panties standing in front of what appears to be a table and chair.
- Image Three depicted Minor Victim nude kneeling on a table while her anus is being digitally penetrated by an unknown individual.
- Image Four depicts Minor Victim nude photographed from the front standing on the floor in front of the table with her breasts and pubic region exposed.
- Image Five depicts Minor Victim sitting on a table naked engaged in masturbation. More specifically, Minor Victim is observed digitally penetrating her vagina.

37. On September 23, 2021, your affiant was contacted by CPD as it relates to the investigation of WOODWARD and the forensic analysis of **SUBJECT DEVICES**. On September 29, 2021, your affiant was briefed on the investigation of WOODWARD as conducted thus far by CPD. Your affiant also took possession of the **SUBJECT DEVICES** which are now currently stored at the Cincinnati FBI Field Office Evidence Control Room located at 2012 Ronald Reagan Drive in Cincinnati, Ohio 45236.

38. Your affiant further confirmed that on September 22, 2015, WOODWARD pled guilty to two counts of Pandering Sexually Oriented Matter Involving a Minor pursuant to ORC 2907.322(A)(1) and two counts of Pandering Sexually Oriented Matter Involving a Minor pursuant to ORC 2907.322(A)(2), all felonies in the second degree. WOODWARD was convicted of these charges in Harrison County, Ohio. According to state records from the case, WOODWARD admitted to reproducing and disseminating images of child pornography. WOODWARD was sentenced to three years of incarceration and was

classified as a Tier II sex offender. WOODWARD was released from custody on or about June 21, 2016 and completed two years of adult probation on or about June 21, 2018.

39. All the **SUBJECT DEVICES** listed in Attachment A were seized from the person or residence of WOODWARD. The **SUBJECT DEVICES** were then transported to the Cadiz Police Department in Cadiz, Ohio and have remained in law enforcement custody since the time they were seized. No forensic examination of the **SUBJECT DEVICES** has been completed thus far and that the **SUBJECT DEVICES** remain in the same state, for purposes of this investigation, as they were at the time they were seized.
40. Based on the information that had been gathered to date by CPD, combined with your affiant's belief that WOODWARD likely possesses the characteristics common to individuals with a sexual interest in minors, as described below, your affiant believes that there is probable cause that the **SUBJECT DEVICES** contain evidence of WOODWARD's child pornography and child exploitation activities.

VII. SEARCH METHODOLOGY TO BE EMPLOYED

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **SUBJECT DEVICES** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans, downloading or copying of the entire device, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. Specifically, such techniques may include, but are not limited to:

- Examination of all of the data contained in any computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items listed in Attachment B;
- Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items in Attachment B;
- Surveying various files, directories and the individual files they contain;
- Opening files in order to determine their contents;
- Scanning storage areas;
- Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are

likely to appear in the evidence described in Attachment B; and/or

- Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

42. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

43. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who have a sexual interest in children and who produce, distribute, and receive child pornography:

- a) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Those who have a sexual interest in children and who produce, distribute, and receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Those who have a sexual interest in children and who produce, distribute, and receive child pornography often times possess and maintain any "hard copies" of child pornographic material that may exist, that is, their pictures, films, video

tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years. More recently, however, it has become more common for people who have a sexual interest in children to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

- d) Likewise, those who have a sexual interest in children and who produce, distribute, and receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e) Those who have a sexual interest in children and who produce, distribute, and receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f) Those who have a sexual interest in children and who produce, distribute, and receive child pornography rarely are able to abstain from engaging in sexual exploitation of children or child pornography activities for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

44. When images and videos of child pornography are produced and stored on computers and related digital media, forensic evidence of the production, distribution, saving, and storage

of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

45. Based upon the conduct of individuals who have a sexual interest in children and who produce, distribute, and receive child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, that they rarely are able to abstain from child pornography activities for a prolonged period of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252, and 2252A– the distribution, transmission, receipt, and/or possession of child pornography, is currently located on the **SUBJECT DEVICES**.

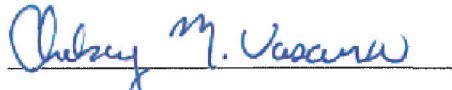
IX. CONCLUSION

46. Based on all the forgoing factual information, there is probable cause to believe that violations of 18 U.S.C. §§ 2252, and 2423 – the distribution, transmission, receipt, and/or possession of child pornography, have been committed and that evidence, fruits and instrumentalities of these offenses will be found within the **SUBJECT DEVICES** listed in Attachment A, which is incorporated herein by reference. Your affiant therefore respectfully requests that the Court issue a search warrant authorizing the search of the **SUBJECT DEVICES** described in Attachment A, and the seizure of the items described in Attachment B.



Andrew D. McCabe
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 12th day of October 2021.



Chelsey M. Vascura
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A
PROPERTY TO BE TO BE SEARCHED

The devices to be searched are the following:

1. One Gateway Laptop Computer, serial number NUUWZMAA004221216BE7614;
2. One Black LG Cellular Telephone.

The items described above were seized from the person WOODWARD or his residence located at 220 East Warren Street in Cadiz, Ohio and are currently being held at the Cincinnati FBI Office located at 2012 Ronald Reagan Drive in Cincinnati, Ohio 45236.

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252 and 2252A – the distribution, transmission, receipt, and/or possession of child pornography, those violations involving William WOODWARD, including:

1. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or online storage or chat programs), utilities, compilers, interpreters, and communications programs.
2. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, and electronic messages,) pertaining to the production, possession, receipt, or distribution of child pornography.
3. In any format and medium, all originals, computer files, copies, and negatives of child pornography and child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to digital files, e-mail messages, chat logs and electronic messages), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by cellular phone or computer, any child pornography.
5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications related to the sexual abuse or exploitation of minors.

6. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider or Electronic Communications Service.
7. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
8. Any and all visual depictions of minors, whether clothed or not, for comparison to any child pornography or child erotica found during the execution of this search warrant or obtained during the course of this investigation.
9. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.
10. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed, posted, and/or traded;
11. Any Internet or cellular telephone communications (including email, social media, etc.) with minors;
12. Evidence of the utilization of peer-to-peer file sharing programs;
13. Evidence of utilization of user names or aliases, email accounts, social media accounts, and online chat programs, and usernames, passwords, and records related to such accounts;
14. Evidence of software that would allow others to control the **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the

presence or absence of security software designed to detect malicious software and evidence of the lack of such malicious software;

15. Evidence indicating the computer user's state of mind as it relates to the crimes under investigation;

16. Evidence that any of the **SUBJECT DEVICES** were attached to any other digital device or digital storage medium;

17. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES**;

18. Passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;

19. Records of or information about Internet Protocol addresses used by the **SUBJECT DEVICES**;

20. Records of or information about any Internet activity occurring on the **SUBJECT DEVICES**, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.